



13W

PTO/SB/21 (02-04)

Approved for use through 07/31/2006. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission

40

Application Number

10/799,215

Filing Date

3/11/2004

First Named Inventor

Kazuomi Olshi

Art Unit

2131

Examiner Name

unknown

Attorney Docket Number

CFA00096US

ENCLOSURES (Check all that apply)

- | | | |
|---|--|---|
| <input type="checkbox"/> Fee Transmittal Form | <input type="checkbox"/> Drawing(s) | <input type="checkbox"/> After Allowance communication to Technology Center (TC) |
| <input type="checkbox"/> Fee Attached | <input type="checkbox"/> Licensing-related Papers | <input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences |
| <input type="checkbox"/> Amendment/Reply | <input type="checkbox"/> Petition | <input type="checkbox"/> Appeal Communication to TC (Appeal Notice, Brief, Reply Brief) |
| <input type="checkbox"/> After Final | <input type="checkbox"/> Petition to Convert to a Provisional Application | <input type="checkbox"/> Proprietary Information |
| <input type="checkbox"/> Affidavits/declaration(s) | <input type="checkbox"/> Power of Attorney, Revocation
Change of Correspondence Address | <input type="checkbox"/> Status Letter |
| <input type="checkbox"/> Extension of Time Request | <input type="checkbox"/> Terminal Disclaimer | <input type="checkbox"/> Other Enclosure(s) (please
Identify below): |
| <input type="checkbox"/> Express Abandonment Request | <input type="checkbox"/> Request for Refund | |
| <input type="checkbox"/> Information Disclosure Statement | <input type="checkbox"/> CD, Number of CD(s) _____ | |
| <input checked="" type="checkbox"/> Certified Copy of Priority Document(s) | <div>Remarks</div> | |
| <input type="checkbox"/> Response to Missing Parts/
Incomplete Application | | |
| <input type="checkbox"/> Response to Missing Parts
under 37 CFR 1.52 or 1.53 | | |

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name
Canon U.S.A., Inc. IP Department
Fidel Nwamu

Signature

Date

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Typed or printed name

Fidel Nwamu

Signature

Date

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 5 月 2 9 日
Date of Application:

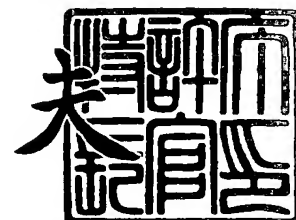
出 願 番 号 特 願 2 0 0 3 - 1 5 2 8 3 4
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 1 5 2 8 3 4]

出 願 人 キヤノン株式会社
Applicant(s):

2 0 0 4 年 6 月 1 4 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康



【書類名】 特許願

【整理番号】 254654

【提出日】 平成15年 5月29日

【あて先】 特許庁長官 太田 信一郎 殿

【国際特許分類】 H04L 12/40

【発明の名称】 特定アドレス使用制限装置

【請求項の数】 7

【発明者】

【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社
内

【氏名】 大石 和臣

【特許出願人】

【識別番号】 000001007

【住所又は居所】 東京都大田区下丸子3丁目30番2号

【氏名又は名称】 キャノン株式会社

【代表者】 御手洗 富士夫

【代理人】

【識別番号】 100090538

【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社
内

【弁理士】

【氏名又は名称】 西山 恵三

【電話番号】 03-3758-2111

【選任した代理人】**【識別番号】** 100096965**【住所又は居所】** 東京都大田区下丸子 3 丁目 3 0 番 2 号キャノン株式会社
社内**【弁理士】****【氏名又は名称】** 内尾 裕一**【電話番号】** 03-3758-2111**【手数料の表示】****【予納台帳番号】** 011224**【納付金額】** 21,000円**【提出物件の目録】****【物件名】** 明細書 1**【物件名】** 図面 1**【物件名】** 要約書 1**【包括委任状番号】** 9908388**【プルーフの要否】** 要

【書類名】 明細書

【発明の名称】 特定アドレス使用制限装置

【特許請求の範囲】

【請求項 1】 他の装置が装置固有の識別子から特定方法で生成したネットワークアドレスの使用を試みていることを検出する検出手段と、

前記試みを検出すると、前記ネットワークアドレスの使用制限を通知する手段とを有することを特徴とする特定アドレス使用制限装置。

【請求項 2】 前記ネットワークアドレスは、Internet Protocol Version 6 (IP v 6) のネットワークアドレスであり、前記装置固有の識別子からネットワークアドレスを生成する特定方法は、IEEE EUI-64 形式のインターフェイス ID を用いてネットワークアドレスを生成する方法であり、前記通知手段は、IP v 6 の Neighbor Discovery Protocol の a multicast Neighbor Advertisement を送信する手段であることを特徴とする前記請求項 1 記載の特定アドレス使用制限装置。

【請求項 3】 他の装置が、装置固有の識別子から特定方法で生成したネットワークアドレスを含むデータを送信したことを検出する検出手段と、

前記送信を検出すると、特定ネットワークアドレスを含むデータの転送を中止する手段とを有することを特徴とする外部ネットワークとの中継を行なう特定アドレス使用制限装置。

【請求項 4】 前記ネットワークアドレスは、Internet Protocol Version 6 (IP v 6) のネットワークアドレスであり、前記装置固有の識別子からネットワークアドレスを生成する特定方法は、IEEE EUI-64 形式のインターフェイス ID を用いてネットワークアドレスを生成する方法であり、前記転送中止手段は、IP v 6 のグローバルアドレスを用いたパケットをネットワーク外部に転送しない手段であることを特徴とする前記請求項 3 記載の特定アドレス使用制限装置。

【請求項 5】 他の装置が装置固有の識別子から特定方法で生成したネットワークアドレスの使用を試みていることを検出し、

前記試みを検出すると、前記ネットワークアドレスの使用制限を通知する手段

とを有することを特徴とする特定アドレス使用制限方法。

【請求項 6】 他の装置が、装置固有の識別子から特定方法で生成したネットワークアドレスを含むデータを送信したことを検出し、

前記送信を検出すると、特定ネットワークアドレスを含むデータの転送を中止する手段とを有することを特徴とする外部ネットワークとの中継方法。

【請求項 7】 請求項 5 又は 6 の方法を実行するプログラム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、特定アドレスの使用を制限する装置に関する。

【 0 0 0 2 】

【従来の技術】

I P v 6 に対応するパーソナル・コンピュータやワークステーションでは、ネットワークとの接続のインターフェイスには通常はイーサネット（R）が用いられ、それが持つ I E E E i d e n t i f i e r （MAC address）を元にして I P v 6 アドレスが生成される。この方法によって生成されたアドレスを I E E E E U I - 6 4 形式の I P v 6 アドレスと呼ぶ。

【 0 0 0 3 】

I P v 6 アドレスには、後述するようにリンクローカルアドレス、サイトローカルアドレスと（集約可能）グローバルアドレスの 3 種類が存在する。

【 0 0 0 4 】

それらの詳細や構成方法などのアドレス体系は、RFC 2373 ‘ ‘IPVersion 6 Addressing Architecture,’ ’ ‘ ‘ RFC 2374 ‘ ‘An IPv6 Aggregatable Global Unicast Address Format,’ ’ RFC 2375 ‘ ‘IPv6 Multicast Address Assignment,’ ’ RFC 2450 ‘ ‘Proposed TLA and NLA Assignment Rule,’ ’ RFC2461 ‘ ‘Neighbor Discovery for IP Version 6 (IPv6),’ ’ RFC 2462 ‘ ‘IPv6 Stateless Address Autoconfiguration,’ ’ 等に記述されている。

【 0 0 0 5 】

ところで、I E E E E U I - 6 4 形式の I P v 6 アドレスのように、I E E

E i d e n t i f i e r (MAC address) 等のハードウェアに 1 対 1 に対応する情報を固定的に用いて生成されたアドレスを使うと、それが装置もしくはその装置のユーザと 1 対 1 に対応する情報とみなされ、そのアドレスを使う通信をモニターされることによりプライバシーが侵害される恐れが強い。

【0006】

この課題に対しては、ランダムな I P v 6 アドレス (正確には interface ID) を生成する方法が、RFC3041 ' ' Privacy Extensions for Stateless Address A utoconfiguration in IPv6,' ' 等において提案されている。生成したランダムな値が既に使われている場合には、それを検出し、別のランダムな値を計算／生成し、ユニークなランダムな値を定めるプロトコル (の拡張) も記述されている。このランダムな I P v 6 アドレスは、t e m p o r a r y a d d r e s s あるいは匿名アドレスと呼ばれる。

【0007】

【発明が解決しようとする課題】

しかし、全ての装置が匿名アドレスを常に使うとは限らない。I E E E E U I - 6 4 形式のアドレスを使うように初期設定されている装置も存在すると考えられ、その装置がそのアドレスを継続使用するとプライバシーが侵害される可能性がある。

【0008】

【課題を解決するための手段】

上記課題を解決するために、本出願に関わる発明は、ローカルなネットワークに設けた特定アドレス使用制限装置が、ネットワーク上の他の装置が I E E E E U I - 6 4 形式のアドレスの使用を試みるか否かを判断し、前記他の装置が I E E E E U I - 6 4 形式のアドレス使用を試みる場合は、そのアドレスが既に使用されている旨のメッセージを送る手段を有する。

【0009】

本手段により、ネットワーク上の装置が I E E E E U I - 6 4 形式のアドレスを使用することを防ぐことができるので、I E E E E U I - 6 4 形式のアドレスを使用した通信をモニターされてプライバシーが侵害される可能性を無くすこ

とができる。

【0010】

上記課題を解決するために、本出願の他の発明では、ローカルなネットワークにおける default gateway が特定アドレス使用制限装置を兼ねる。前記制限装置は、ネットワーク上の他の装置が IEEE EUI-64 形式のアドレスを含むデータを送信するか否かを判断し、前記他の装置が IEEE EUI-64 形式のアドレスを含むデータを送信する場合は、そのアドレスを記録し、そのアドレスを含むデータをネットワーク外部へ転送しないように処理する制御手段を有する。

【0011】

本手段により、ネットワーク上の他の装置が IEEE EUI-64 形式のアドレスを使用してネットワーク外部と通信することを防ぐことができるので、IEEE EUI-64 形式のアドレスを使用した通信をモニターされてプライバシーが侵害される可能性を無くすることができる。

【0012】

【発明の実施の形態】

（第1の実施の形態）

本実施の形態では、ホストがイーサネット（R）の LAN 経由でインターネットと接続する場合を説明する。最初に現状を説明し、その後に本発明の実施の形態を説明する。

【0013】

図2は、本発明が適用される接続環境（ホストがイーサネット（R）の LAN 経由でインターネットと接続する環境）を模式的に示したものである。

【0014】

図2は、LANに接続されたホスト204、205、206が gateway 202 経由でインターネット201にアクセスする環境を示す。本実施の形態では、各ホストはリンク207で接続するものとし、具体的にはイーサネット（R）であるとする。208もリンクである。リンクとは、それに接続された装置がそれを介して通信することができる設備もしくはメディアであり、IP層の下側

に接する。リンクにはイーサネット（R）の他に、PPPリンク、X.25、フレームリレー、ATMネットワークがある。リンクに接続されたIPv6装置をノードと呼ぶ。203はDHCPサーバーである。

【0015】

ノードの内部構成の典型例を図3に示す。

【0016】

ノードには、ルーターとホストがあり、ルーターは自分宛ではないパケットを転送するがホストは転送しない。図3からわかるように、ノード300は、ネットワーク・インターフェイス301、302、CPU303、ROM304、RAM305、HD（ハードディスク）306、電源307、キーボード／ポインティングデバイスのインターフェイス308、モニターのインターフェイス309、バス310等を有する計算機である。

【0017】

ルーターは複数のインターフェイス301、302を持つのに対し、ホストは多くの場合は一つのインターフェイス301を持つ。ネットワーク・インターフェイス301は、リンク207に接続され、リンク207に接続された他のノードと通信する。

【0018】

ホスト204、205、206は、ネットワーク・インターフェイス301により、リンク207を介して、リンク207に接続された他のノード、あるいは、更に、ゲートウェイ202を介して、インターネット201上のサイトと通信する。ゲートウェイ202（ルーター）においては、ネットワーク・インターフェイス301は、リンク207に接続され、それを介してリンク上の他の装置と通信し、ネットワーク・インターフェイス302はリンク208に接続され、それを介してインターネット201と接続され、それらを介してインターネット上のノードと通信する。なお、ノードによってはHDを持たないものもある。

【0019】

なお以下の処理内容（手順）は、装置もしくはプログラムとして実現される。すなわち、装置で実現する形態では、その装置を有するノード300が、以下の

処理内容（手順）を実行する。また、プログラムとして実現する形態では、そのプログラムが R O M 3 0 4 もしくは H D 3 0 6 に格納されたノードが、以下の処理内容（手順）を実行する。例えば、プログラムとして実現される場合は、そのプログラムを C P U 3 0 3 が読み込み、必要に応じて R A M 3 0 5 を計算のための空間として利用しながらバス 3 1 0 を介してインターフェイス 3 0 1、3 0 2 にアドレスを割当て、というような動作を行なう。

【0 0 2 0】

本実施の形態のイーサネット（R）LAN環境で各ホストがI P v 6 グローバルアドレスのプレフィックスやd e f a u l t g a t e w a yのアドレスを取得するプロトコルの仕組みを簡単に説明し、その次に本発明を適用した具体的な実施の形態を説明する。

【0 0 2 1】

典型的なI P v 6 アドレスはp r e f i xとi n t e r f a c e I Dからなり、p r e f i xが上位6 4 ビット、i n t e r f a c e I Dが下位6 4 ビットである。i n t e r f a c e I Dは、イーサネット（R）・インターフェイスのM A C a d d r e s s 4 8 ビットを元にして以下のように生成される。

【0 0 2 2】

イーサネット（R）のI E E E i d e n t i f i e r（M A C a d d r e s s）は、6 バイト長のアドレスで、先頭の3 バイトは製造ベンダーコードとしてI E E Eによって管理・割当てがされている。残り3 バイトは各ベンダーに管理が任されており、重複が起こらないように割当てがされる。図4にイーサネット（R）のM A C a d d r e s sの構成を示す。各四角は1 バイト（8 ビット）のデータを示し、左から3 バイトは製造ベンダーコード、残り3 バイトはベンダーが管理するコードとなっている。ベンダーが管理するコードはイーサネット（R）・カード毎に異なるように振られるので、イーサネット（R）・カード毎に世界で唯一のアドレスが対応し、イーサネット（R）上でのデータの送受信の際にアドレスとして利用される。

【0 0 2 3】

イーサネット（R）のM A C a d d r e s s（図4参照）を3 バイトずつに

分割し、中間に16進数の「FFFE」をはさみ、先頭から7ビット目を1にする。これを図5に示す。図5のC1'は、図4のC1の先頭から7ビット目を1にしたものを表す。このようにして生成された、図5の構成の64ビット・データをIEEE EUI-64形式のinterface IDと呼ぶ。IEEE EUI-64形式のinterface IDから生成されたIPv6アドレスをIEEE EUI-64形式のIPv6アドレスと呼ぶ。

【0024】

次に、図3のノードが、電源を入られたあるいはリブートされた場合に行なう動作のフローチャートを図8に示す。この動作はDAD (Duplicate Address Detection) と呼ばれる。以下では図8の流れに沿って処理内容を説明する。

【0025】

ステップS801でノード300が電源を入られたあるいはリブートされた後、まずネットワーク・インターフェイス301のイーサネット (R) のMAC address (図4参照) からinterface ID (図5参照) を作成し、それをtentative link-local address (図6参照) とする (ステップS802)。

【0026】

次に、そのtentative link-local addressがリンク207上で一意かどうかを判断するために、ノード300は以下の処理を行なう。

【0027】

最初に、インターフェイス301の初期設定をする。すなわち、インターフェイス301に、all-nodes multicast address (FF02::1) とそのtentative link-local addressのsolicited-node multicast addressを割当て (図7参照)。つまり、そのインターフェイス301がall-nodes multicast address宛のパケットあるいはそのtentative link-local addressのsolicited-node multicast address宛のパケットを見つけたときはそ

れを自分のインターフェイス宛のパケットとして受け取る。

【0028】

前者 (all-nodes multicast address) を割当てることによって、既にその tentative link-local address を使っている他のノードからのデータを受信することが可能になる。また、後者 (その tentative link-local address の solicited-node multicast address) を割当てることによって、同じ tentative link-local address を同時に使おうとしている他のノードの存在を検出することが可能になる。

【0029】

ある tentative link-local address の solicited-node multicast address とは、RFC 2461 の page 91 に定義されているように、tentative link-local address の下位 24 ビットをプレフィックス FF02:0:0:0:1:FF00::/104 に付加したデータであり、link-local scope multicast address である。図6と図7にそれらの関係を示す。以上のアドレス割当てが図8のステップ S803 である。

【0030】

次に Neighbor Solicitation message を作る。Neighbor Solicitation message の Target Address (ターゲットアドレス) には判断対象の tentative link-local address を、IP Source (送信元アドレス) には unspecified address (128 ビット全てが 0) を、IP destination (宛先アドレス) には判断対象の tentative link-local address の solicited-node multicast address を設定する。

【0031】

このNeighbor Solicitation messageをRetransTimerミリ秒間隔でDupAddrDetectTransmits個イーサネット(R) 207に送出する。図8のステップS804がこの処理である。

【0032】

Neighbor Solicitation messageを受け取ったノードは、その送信元アドレスが unspecified addressならば、そのmessageがDADを行っているノードからのデータであることと判断する。

【0033】

同時に複数のノードが同じアドレスを対象としてDADをしている場合は、自分が送ったNeighbor Solicitation messages以外にも、同じアドレスをTarget Addressに含むNeighbor Solicitation messagesを受け取る（自分が送ったNeighbor Solicitation messageと、同時にそのアドレスを対象としてDADをしている他のノードが送ったNeighbor Solicitation messageを受け取る）ので、重複していることがわかる。その場合にはどのノードもそのアドレスは使わない。

【0034】

なお、受け取ったNeighbor Solicitation messageが、自分が送ったもの（マルチキャストの packets をループバックしているため）であるならば、他にそれを使っているあるいは使おうとしているノードが存在することを示さない。自分が送ったNeighbor Solicitation messageに加えて、同じアドレスをTarget Addressに含むNeighbor Solicitation messagesを受け取った場合に、同時に複数のノードが同じアドレスを対象としてDADをしていると判断する。

【0035】

一方、Neighbor Solicitation messageを受け

取ったノードが、そのmessageのTarget Address（ターゲットアドレス）に含まれるアドレスを既に使っていれば、Target Addressにそのtentative link-local addressが設定されたa multicast Neighbor Advertisementをall-nodes multicast address宛てに返す。従って、Neighbor Solicitation messageを送ったノードがall-nodes multicast address宛てのa multicast Neighbor Advertisementを受け取り、そのtarget addressが（判断対象の）tentative addressである場合（図8のS805ステップの「はい」の場合）は判断対象のtentative addressが唯一ではない（つまり、重複している）。

【0036】

以上のDADの結果、判断対象のtentative link-local addressがリンク207上で唯一であることが確認された（図8のS805ステップの「いいえ」の場合）ならば、そのアドレスをリンクローカルアドレスとしてインターフェイス301に割当てて。これが図8のステップS806である。以上でDADは終了する。

【0037】

以上に説明した図8の動作は図2のgateway 202、DHCP server 203、ホスト204、ホスト205、ホスト206のそれぞれが実行することができる。

【0038】

図2のホスト、例えばホスト206は、リンクローカルアドレスをインターフェイス301に割当てたら、次はサイトローカルアドレスやグローバルアドレスを決定するために必要な情報（Router Advertisementと呼ばれる）を入手することを試みる。

【0039】

この動作を図9に示す。gateway 202が、Router Adver

t i s e m e n t を送る場合を説明する。g a t e w a y 2 0 2 は通常はルーターと呼ばれるので以下ではルーター 2 0 2 と記す。ルーター 2 0 2 は管理者によって必要な設定が行われ、R o u t e r A d v e r t i s e m e n t を定期的にリンク 2 0 7 に送っている。ホスト 2 0 6 が R o u t e r A d v e r t i s e m e n t を早く入手したい場合は、ホスト 2 0 6 は R o u t e r S o l i c i t a t i o n と呼ばれるデータをルーター 2 0 2 に送る。ホスト 2 0 6 はリンクローカルアドレスを割当てた直後にはルーター 2 0 2 の存在はわからないので、実際には R o u t e r S o l i c i t a t i o n はリンク上のルーター全てに対するマルチキャストとして送られる。図 9 のステップ S 9 0 1 はこの処理を示す。

【0040】

R o u t e r S o l i c i t a t i o n を受け取ったルーター 2 0 2 は R o u t e r A d v e r t i s e m e n t を送る。図 9 のステップ S 9 0 2 の「はい」の場合に示すように、S t a t e l e s s a d d r e s s a u t o c o n f i g u r a t i o n のみを指定する R o u t e r A d v e r t i s e m e n t を受け取ったホスト 2 0 6 は、そのメッセージに含まれるプレフィックスの有効性（既にその装置によって使われていないこと等）を確認し、それ（ら）にインターフェイス ID を付加して作ったアドレスを、サイトローカルアドレスあるいはグローバルアドレスとし、インターフェイス 3 0 1 に割当てて。図 9 のステップ S 9 0 3 がこの処理である。

【0041】

図 9 のステップ S 9 0 2 の「いいえ」の場合に示すように、ホスト 2 0 6 が s t a t e l e s s a d d r e s s a u t o c o n f i g u r a t i o n のみを指定する R o u t e r A d v e r t i s e m e n t を受け取らなかった場合は、次の二つの場合に分けられる。S t a t e l e s s a d d r e s s a u t o c o n f i g u r a t i o n と s t a t e f u l a d d r e s s a u t o c o n f i g u r a t i o n の両方を指定する R o u t e r A d v e r t i s e m e n t を受け取った場合（ステップ S 9 0 4 のはいの場合）と、R o u t e r A d v e r t i s e m e n t を何も受け取らなかった場合（ステップ S 9

04のいいえの場合)である。

【0042】

後者の場合は `stateful address autoconfiguration`、すなわちDHCPv6のみを実行する。これがステップS906であり、その基本的な動作フローチャートを図10に示す。

【0043】

なお、`stateful address autoconfiguration`においてやり取りされるメッセージの内容や形式等の詳細は、“`draft-ietf-dhc-dhcpv6-23.txt`”もしくはその改訂版に説明されている。以下では図10の番号に沿って基本的な動作の流れを説明する。

【0044】

DHCPサーバー203は管理者によって必要な設定が行われている。具体的には、ノードとして自分のリンクローカルアドレスをインターフェイス301に割当ててあり、DHCPサーバーとして振る舞うために必要なサイトローカルアドレスもしくはグローバルアドレスのためのプレフィックス等が設定されている。

【0045】

図10のステップS1001で、ホスト204は、DHCPサーバーにDHCP `Solicit Message`を送る。ホスト206はどこにDHCPサーバーが存在するのかわからないので、DHCPサーバーに対するマルチキャストとしてリンク207に送出する。ホスト206の接続されているリンク207とは異なるリンク（図示せず）にDHCPサーバーがいる場合には、DHCP `Solicit Message`は、実際にはDHCPリレー（図示せず）によって中継されてDHCPサーバー203に届く。

【0046】

DHCP `Solicit Message`を受け取ったDHCPサーバー203はそれに対する返答としてDHCP `Advertise Message`をホスト206に返す。これは（別リンクの場合はDHCPリレーによって中継されて）ホスト206に届く。これがステップS1002である。この時点でホ

スト 206 は DHCP サーバー 203 のアドレスがわかる。

【0047】

次にステップ S1003 でホスト 206 は DHCP Request Message を DHCP サーバー 203 に送る。DHCP サーバー 203 は DHCP Request Message を受け取ると、ステップ S1004 で DHCP Reply Message をホスト 206 に送る。

【0048】

ステップ S1004 で DHCP Reply Message 受け取ったホスト 206 は、それからサイトローカルアドレスもしくはグローバルアドレスがわかるので、そのアドレスの中の interface ID が重複しているか否かを確認するために、DAD 処理に必要な処理を行なう。つまり、インターフェイス 301 に前述のマルチキャストアドレス等を設定する。これがステップ S1005 である。

【0049】

次に、ステップ S1006 で Neighbor Solicitation Message を送り、Neighbor Advertisement Message を受け取るかどうかをステップ S1007 で判断する。受け取った場合はそのアドレスが重複しているので、別のアドレスを DHCP サーバー 203 から受け取るためにステップ S1003 に戻り、同じ処理を繰り返す。

【0050】

ホスト 206 は、図 10 のステップ S1007 で Neighbor Advertisement Message を受け取らなかった場合はそのアドレスは重複していないので、ステップ S1008 でそのアドレスをインターフェイス 301 に割当てて。

【0051】

以上で図 9 のステップ S906 が終わる。ステップ S904 で Router Advertisement を何も受け取らなかった場合はこれで正常終了する。

【0052】

ステップS902でstateless address autoconfigurationとstateful address autoconfigurationの両方を指定するRouter Advertisementを受け取った場合は、ステップS905でstateless address autoconfigurationとstateful address autoconfigurationの両方を行なう。処理内容はステップS903とS906と同じである。

【0053】

以上のようにして、イーサネット（R）をインターフェイスとして持つホスト206はstateless address autoconfigurationとstateful address autoconfiguration（DHCPv6）を任意の組み合わせで適用して、リンクローカルアドレス、サイトローカルアドレス、グローバルアドレス、default gateway等を自動設定することができる。

【0054】

匿名アドレスを使う場合は、以上のプロトコルが次のように拡張される。図9のステップS903あるいはステップS905において、ホスト206はRouter Advertisementを受け取り、それに含まれるプレフィックスの有効性（既にその装置によって使われていないこと等）を確認し、それ（ら）にインターフェイスIDを付加して作ったアドレスを、サイトローカルアドレスあるいはグローバルアドレスとし、インターフェイス301に割当ててゐる。この際に、IEEE EUI-64形式で生成したinterface IDのみではなく、ランダムなinterface IDにも同じ処理を行なう。ランダムなinterface IDの生成方法は後述する。

【0055】

新しい匿名アドレスはプレフィックスにランダムなinterface IDを付加して作られる。ホスト206が既にインターフェイスに割当ててゐるアドレスと新しい匿名アドレスが同じ場合は、新しいランダムなinterface IDを生成し、新しい匿名アドレスを生成する。

【0 0 5 6】

次に、ホスト 2 0 6 は匿名アドレスを対象に D A D を実行する。D A D によって、他の装置がその匿名アドレスを既に使用していることがわかった場合は、新しい匿名アドレスを生成する。最大 5 回まで繰り返し、その結果一意の匿名アドレスを得ることが出来ない場合は、ホスト 2 0 6 はシステム・エラーをログ（記録）に残し、匿名アドレスを生成することをあきらめる。

【0 0 5 7】

ランダムな `i n t e r f a c e I D` は、`M D 5 m e s s a g e d i g e s t` を使って生成される。`M D 5` とは任意の入力から、ランダムな 1 2 8 ビットを出力する関数である。`R F C 3 0 4 1` の方法では 1 2 8 ビットが入力される。この入力 1 2 8 ビットは上位 6 4 ビットと下位 6 4 ビットから次のように構成される。`i n t e r f a c e I D` を上位 6 4 ビットとする。何らかの方法で生成したランダムな値 6 4 ビットあるいは前回の `M D 5` の計算結果の下位 6 4 ビットを、入力 1 2 8 ビットの下位 6 4 ビットとする。この 1 2 8 ビットを入力として `M D 5 m e s s a g e d i g e s t` を計算し、その計算結果 1 2 8 ビットの上位 6 4 ビットを取り出す。取り出した 6 4 ビットの左から 7 ビット目をゼロにした 6 4 ビットを `i n t e r f a c e I D` とする。計算結果の下位 6 4 ビットは、次の `M D 5` の計算に用いるため、記録しておく。

【0 0 5 8】

次に本発明の実施の形態を説明する。上述した動作（プロトコル）を利用して、`I E E E E U I - 6 4` 形式のアドレスを使用させないプロトコルを説明する。

【0 0 5 9】

なお、`I P` の下層に位置するデータリンク層の通信は、イーサネット（`R`）の場合、イーサネット（`R`）・インターフェイスの `M A C a d d r e s s` を識別子とする放送型パケット通信である。従って、イーサネット（`R`）にアクセスできる装置は通信される全てのパケットを観測でき、各パケットの送信元 `M A C a d d r e s s` と宛先 `M A C a d d r e s s` を取得することができる。

【0 0 6 0】

本形態の特定アドレス使用制限装置の動作を、図1にそって説明する。例として、ホスト206がIEEE EUI-64形式のアドレスの使用を試みる場合を説明する。なお以下の処理内容（手順）は、装置もしくはプログラムとして実現される。プログラムとして実現する形態では、そのプログラムがROM304もしくはHD306に格納されたノードが、以下の処理内容（手順）を実行する。図1は、このプログラムの主要部を示す。

【0061】

この場合、リンク207に接続されているならば、どのIPv6装置であってもホスト206のMAC addressを取得できるので、gateway 202、DHCP server 203、ホスト204、ホスト205（およびホスト206）のいずれも特定アドレス使用制限装置として動作可能である。

【0062】

IPv6装置が使用希望または使用するIPv6アドレスが匿名アドレス（temporary address）であるか否かを、その装置のデータリンク層のMACアドレスからIEEE EUI-64形式で生成したアドレスと比較して判断するノードまたはルーター202を、装置206と同じサブネット207に設ける。IEEE EUI-64形式のアドレスを使用希望する場合はそれが既に使用されている旨のメッセージをノードが送出して、装置にそのアドレスを使用させない。

【0063】

すなわち、電源を入れたあるいはリブートされたホスト206がDADを実行する。このDADにおいて、Neighbor Solicitation messageを受け取った特定アドレス使用制限装置は、ステップS101で、そのTarget Addressを取り出し、それが自身のアドレスと一致するか否かを判断し、一致する場合はステップS107に、一致しない場合はステップS102に進む。

【0064】

ステップS102で、Target Addressの下位64ビット（interface ID）を取り出す。

【0065】

ステップS103で、取り出したinterface IDの左から25～40ビットが0xFFFEであるか否かを判断し、0xFFFEでない場合は処理を終了し、0xFFFEである場合はステップS104に進む。

【0066】

ステップS104で、取り出したinterface IDの左から7ビット目が1であるか否かを判断し、1でない場合は処理を終了し、1の場合はステップS105に進む。

【0067】

ステップS105で、Neighbor Solicitation messageを含むイーサネット(R)・パケットの送信元MAC address (送信元のデータリンク層の識別子であり、送信元の装置固有の識別子である)を取り出す。

【0068】

ステップS106で、送信元MAC address (送信元の装置固有の識別子)からIEEE EUI-64形式で生成した64ビットデータと、ステップS102で取り出したinterface IDとが一致するか否かを判断する。一致する場合はステップS107に進み、一致しない場合は終了する。

【0069】

ステップS107でIPv6のNeighbor Discovery Protocolのa multicast Neighbor Advertisementを送る。

【0070】

以上の処理が行なわれると、ホスト206がIEEE EUI-64形式のinterface IDとは異なるinterface IDを使おうとするときはa multicast Neighbor Advertisementを受け取らないので、それから生成されるIPv6アドレスを使える。

【0071】

一方、IEEE EUI-64形式のinterface IDを使おうとする

と、a multicast Neighbor Advertisementを受け取るのでそのinterface IDおよびそれから生成されるIPv6アドレスを使えない（可能ならば、他のIPv6アドレスを生成して、用いることになる）。

【0072】

すなわち、送信元であるホスト206が、送信元MACアドレス（送信元のデータリンク層の識別子であり、送信元の装置固有の識別子である）から特定方法で生成したネットワークアドレス（IEEE EUI-64形式のinterface IDから生成したIPv6アドレス）の使用を試みると、特定アドレス使用制限装置は、その試みを検出する。そして、そのネットワークアドレスが使用されていることを示すメッセージであるa multicast Neighbor Advertisementを送信することにより、ホスト206にそのネットワークアドレスの使用制限を通知する。

【0073】

従って、プライバシーを侵害される可能性をなくすることができる。

【0074】

（第2の実施の形態）

本実施の形態では、IEEE EUI-64形式のinterface IDから生成されたアドレスは使用されるが、それを使ってネットワーク外部とは通信させないことにより、プライバシーを侵害されないようにする。

【0075】

第1の実施の形態では、IEEE EUI-64形式のinterface IDを一切使わせないようになっているので、他のinterface IDを生成する手段を持たないIPv6装置は、アドレスを持つことが出来ない。設定の変更をネットワーク経由でのみ行なえるIPv6装置も考えられるので、本実施の形態では、IEEE EUI-64形式のインターフェイスIDから生成したリンクローカルアドレスを使えるようにし、しかし、IEEE EUI-64形式のインターフェイスIDから生成したグローバルアドレスは使えないようにする特定アドレス使用制限装置を提供する。

【0076】

本実施の形態における特定アドレス使用制限装置は、図2における gateway 202（ルーター）として実現される。図11にそって、その動作を説明する。なお以下の処理内容（手順）は、装置もしくはプログラムとして実現される。プログラムとして実現する形態では、そのプログラムがROM304もしくはHD306に格納されたノードが、以下の処理内容（手順）を実行する。図11は、このプログラムの主要部を示す。特定アドレス使用制限装置は、リストを生成・管理しているものとする。このリストは、RAM305に格納される。このリストには、後述のS1007で、アドレスが登録される。

【0077】

IPv6装置が使用希望または使用するIPv6アドレスが匿名アドレス（temporary address）であるか否かを、その装置のデータリンク層のMACアドレスからIEEE EUI-64形式で生成したアドレスと比較して判断するノードまたはルーター202を、装置と同じサブネット207に設ける。そのアドレスを含むパケットか否かをルーター202が判断して、当該パケットの場合は破棄し、ネットワーク207外部へ転送しない。

【0078】

特定アドレス使用制限装置は、リンク207上のIPv6装置（例えば、ホスト206）から外部ネットワーク201へ転送するものとして受け取ったIPv6パケットを対象に、次の処理を行なう。外部ネットワーク201へ転送するものとして受け取ったIPv6パケットとは、destination addressが、外部ネットワーク201上のアドレスであるIPv6パケットである。

【0079】

ステップS1001で、対象とするIPv6パケットのsource addressを取り出し、それがリストに登録されているか否かを判定する。登録されている場合は、ステップS1008に進む。登録されていない場合は、ステップS1002に進む。

【0080】

ステップS1002で、対象IPv6パケットのsource addressの下位64ビット（インターフェイスID）を取り出す。取り出したinterface IDの左から25～40ビットが0xFFFEであるか否かを判断し、0xFFFEでない場合はステップS1009に進み、0xFFFEである場合はステップS1004に進む。

【0081】

ステップS1004で、取り出したinterface IDの左から7ビット目が1であるか否かを判断し、1でない場合はステップS1009に進み、1の場合はステップ1005に進む。

【0082】

ステップ1005で、対象のIPv6パケットを含むイーサネット（R）・パケットの送信元MAC addressを取り出す。

【0083】

ステップ1006で、送信元MAC addressからIEEE EUI-64形式で生成した64ビットデータと、ステップ1002で取り出したinterface IDとが一致するか否かを判断する。一致する場合はステップ1007に進み、一致しない場合はステップS1009に進む。

【0084】

ステップ1007で対象IPv6パケットのsource addressをリストに登録し、ステップS1008に進む。したがって、このアドレスがリストに登録された以降、外部ネットワークへのパケットのソースアドレス（発信元アドレス）が、このアドレスであった場合には、S1002からS1007の処理を行なうことなく、S1001からS1008へ進む。

【0085】

ステップS1008で、対象IPv6パケットを破棄し、終了する。

【0086】

ステップS1009で、対象IPv6パケットを外部ネットワーク201に転送し、終了する。

【0087】

以上の動作から明らかなように、IEEE EUI-64形式の interface ID から生成されたグローバルアドレスを source address とする IPv6 パケットは破棄されるので、外部ネットワーク 201 に転送されない。

【0088】

一方、IEEE EUI-64 形式とは異なるインターフェイス ID から生成されたグローバルアドレスを source address とする IPv6 パケットは、外部ネットワーク 201 に転送される。

【0089】

すなわち、送信元であるホスト 206 の MAC アドレス（データリンク層の識別子であり、装置固有の識別子である）から特定方法で生成したネットワークアドレス（IEEE EUI-64 形式のインターフェイス ID から生成した IPv6 アドレス）を含むデータの送信を、特定アドレス使用制限装置が検出し、そのデータの転送を中止する。

【0090】

従って、プライバシーを侵害される可能性をなくすることができる。

【0091】

【発明の効果】

本発明によれば、プライバシーの侵害を防ぐことができる。

【0092】

IPv6 ネットワークにおいて、特定方法、例えば IEEE EUI-64 形式で interface ID を生成する装置、あるいは IEEE EUI-64 形式で生成された interface ID から IPv6 アドレスを生成する装置が、その interface ID あるいはその IPv6 アドレスを使用できないようにすることができる。従って、その IPv6 アドレスを使用することによりプライバシーを侵害される可能性をなくす効果が得られる。

【0093】

これにより、IEEE EUI-64 形式で生成された interface ID を使用してしまうことがなくなり、IPv6 装置およびそのユーザのプライバ

シを保護できる。

【0094】

また、プライバシーが侵害される恐れがあるアドレスを用いて、ネットワーク外部とは通信できないようにすることができる。

【0095】

IEEE EUI-64形式のアドレスを使用することは可能だが、それを用いてネットワーク外部とは通信できないようにすることができる。

【0096】

これにより、IEEE EUI-64形式のアドレスを使ってネットワーク内部の通信は行なえるので、ネットワーク設定が簡便であるというIPv6がそもそも持つ特徴を維持しながら、IEEE EUI-64形式で生成されたinterface IDを不用意に使用してしまうことはなくなるので、IPv6装置のユーザの使い勝手を悪くせずにプライバシーを保護できる。

【0097】

対象とするIPv6装置そのものにはいかなる変更も加えないので、既存のIPv6装置を対象に上記効果を得ることができる。

【図面の簡単な説明】

【図1】

アドレス判断の動作フローチャートである。

【図2】

イーサネット(R) LANの模式図である。

【図3】

ノードの構成図である。

【図4】

イーサネット(R)のMAC addressの構成図である。

【図5】

interface IDの構成図である。

【図6】

tentative link-local addressの構成図で

ある。

【図 7】

ある tentative link-local address の solicited-node multicast address の構成図である。

【図 8】

ホストが DAD を終えるまでの動作を説明するフローチャート図である。

【図 9】

ホストがアドレス自動設定を終えるまでの動作を説明するフローチャート図である。

【図 10】

ホストが DHCP でアドレスを取得するまでの動作フローチャート図である。

【図 11】

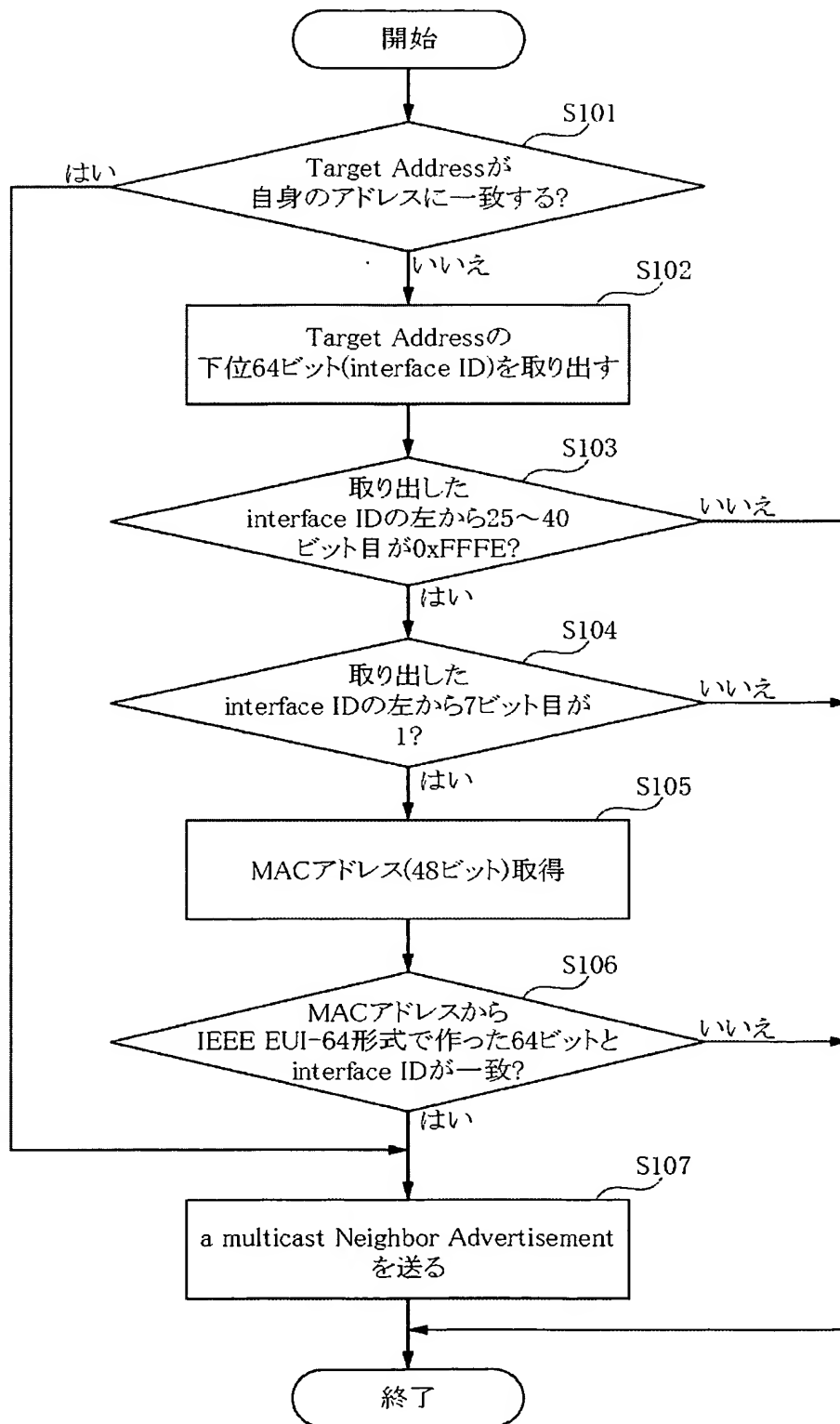
転送判断の動作フローチャートである。

【符号の説明】

- 201 インターネット
- 202 gateway
- 203 DHCP サーバー
- 204 ホスト
- 205 ホスト
- 206 ホスト
- 207 リンク
- 208 リンク

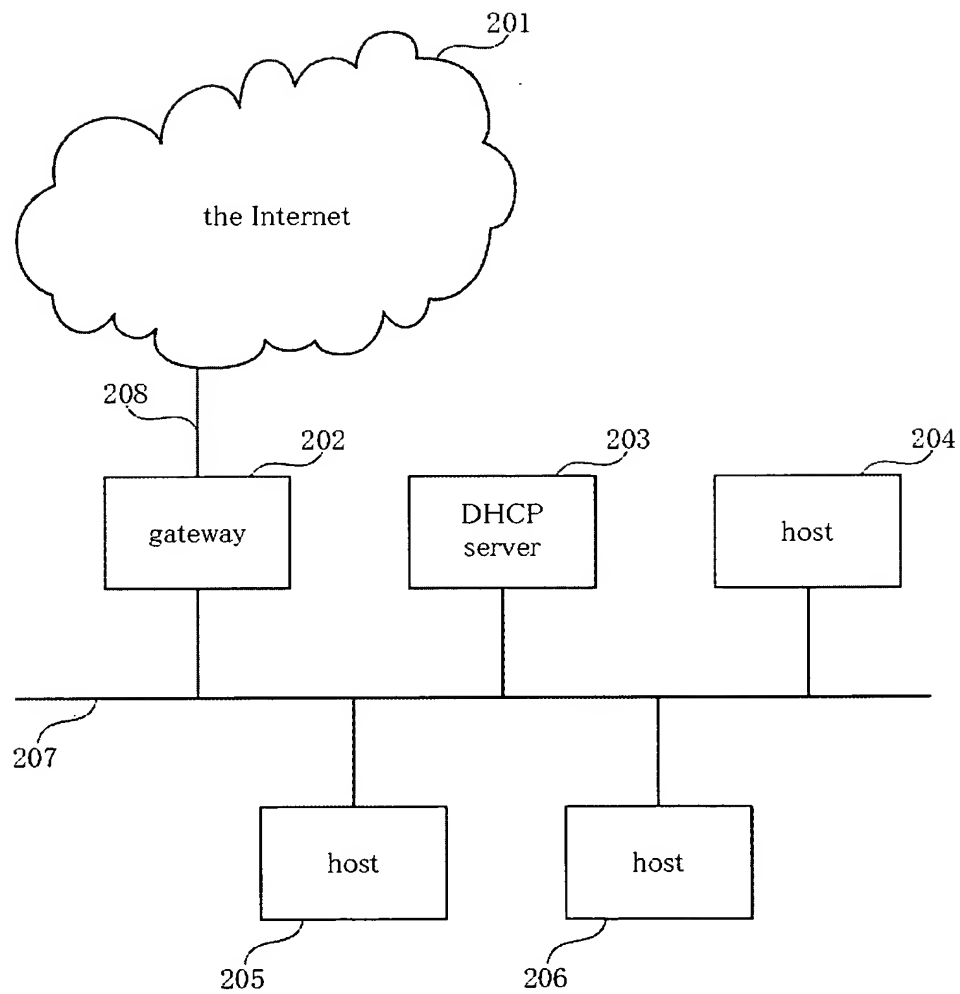
【書類名】 図面

【図 1】



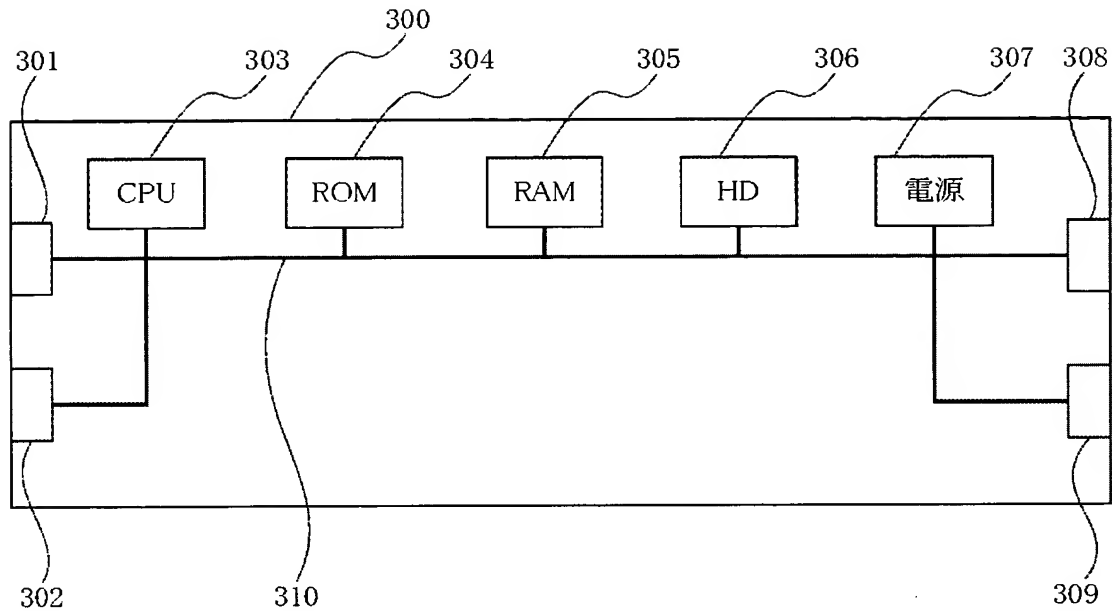
アドレス判断の動作フローチャート

【図 2】



イーサネットLANの模式図

【図 3】



ノードの構成

- 300 ノード筐体
- 301 ネットワーク・インターフェイス
- 302 ネットワーク・インターフェイス
- 303 CPU
- 304 ROM
- 305 RAM
- 306 HD(ハードディスク)
- 307 電源
- 308 キーボード/ポインティングデバイスのインターフェイス
- 309 モニタのインターフェイス
- 310 バス

【図 4】

C1	C2	C3	M1	M2	M3
----	----	----	----	----	----

イーサネットのMACアドレスの構成

【図 5】

C1'	C2	C3	0xFF	0xFE	M1	M2	M3
-----	----	----	------	------	----	----	----

インターフェイスIDの構成

【図 6】

0xFE	0x80	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	C1'	C2	C3	0xFF	0xFE	M1	M2	M3
------	------	-----	-----	-----	-----	-----	-----	-----	-----	-----	----	----	------	------	----	----	----

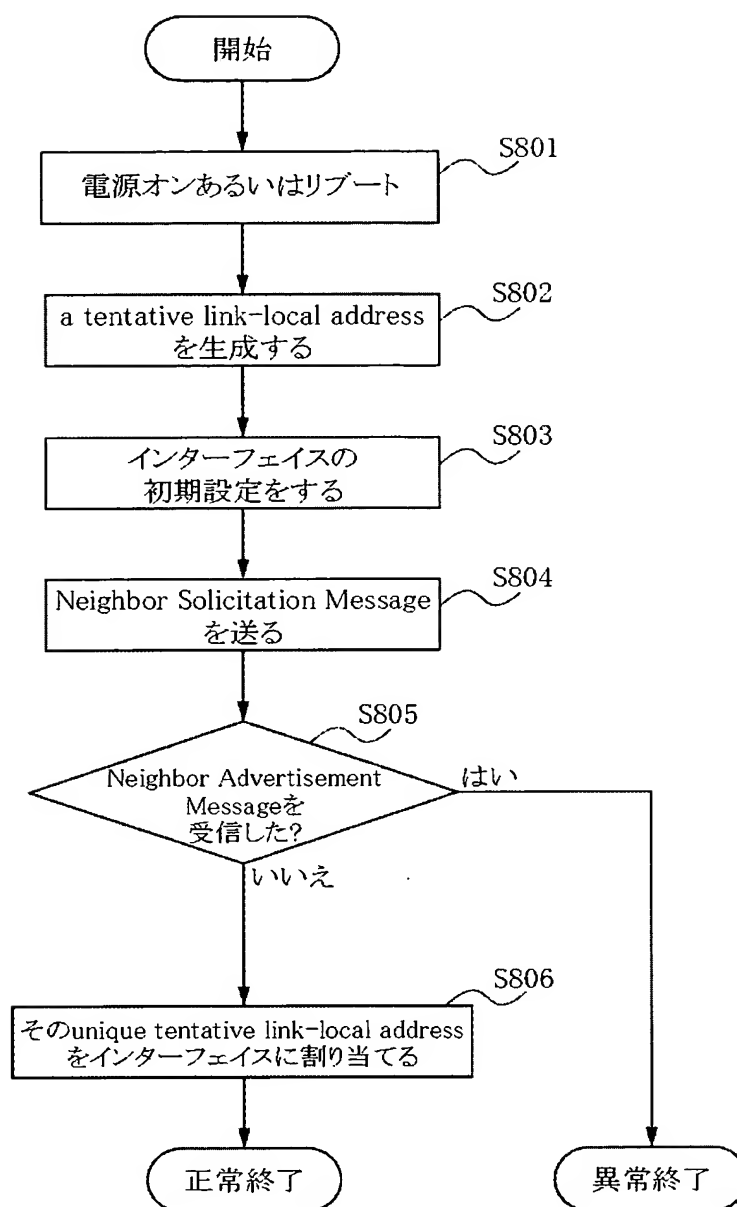
a tentative link-local addressの構成

【図 7】

0xFF	0x02	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x1	0xFF	M1	M2	M3
------	------	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	------	----	----	----

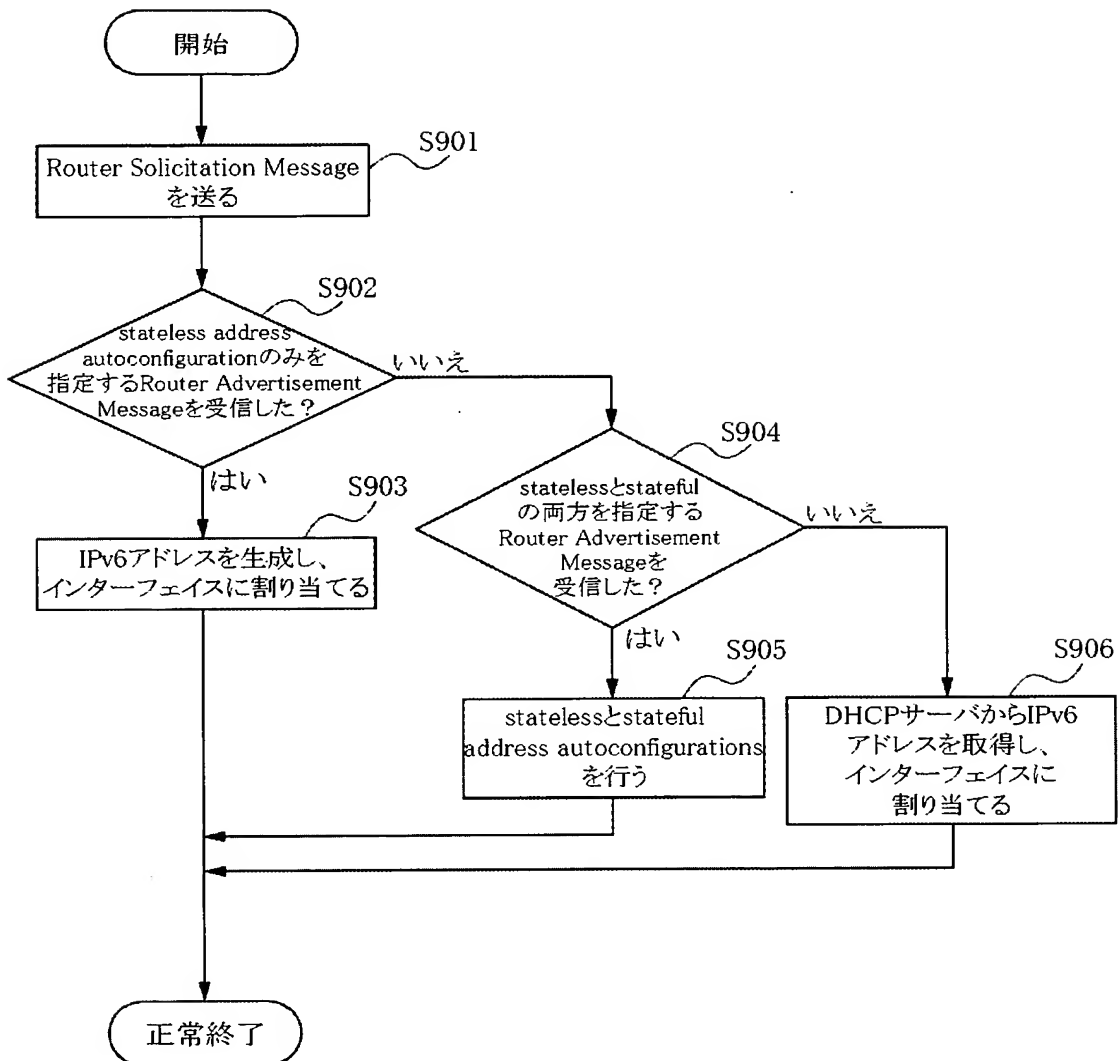
ある tentative link-local address の solicitend-node multicast address の構成

【図 8】



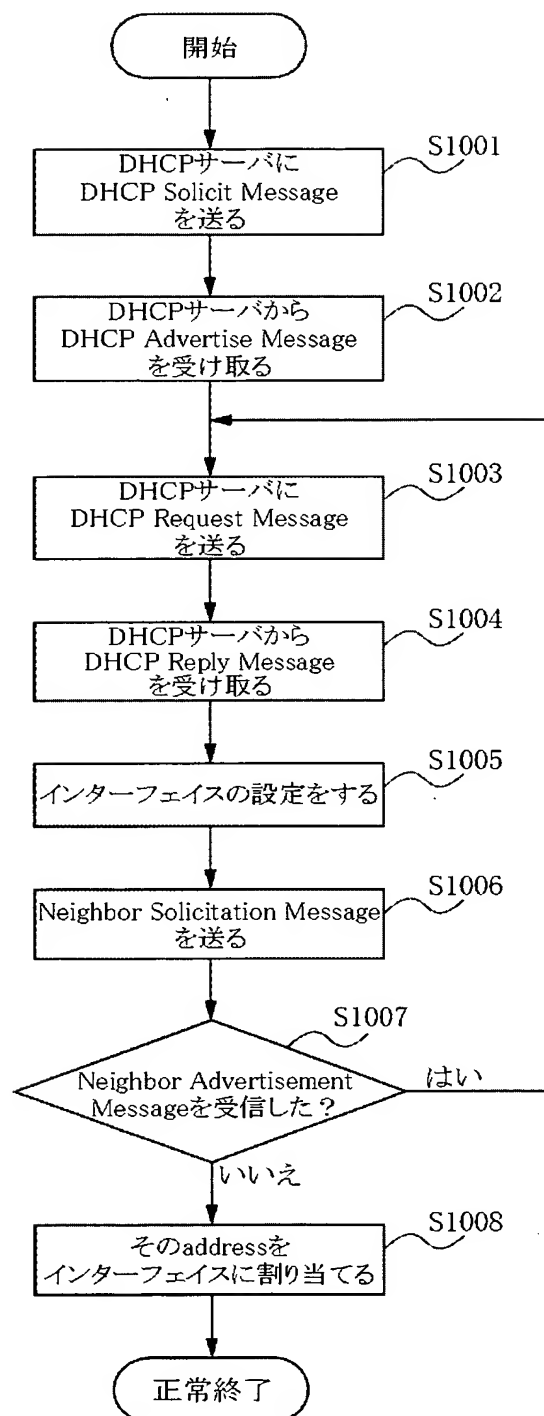
ホストがDADを終えるまでの動作フローチャート

【図 9】



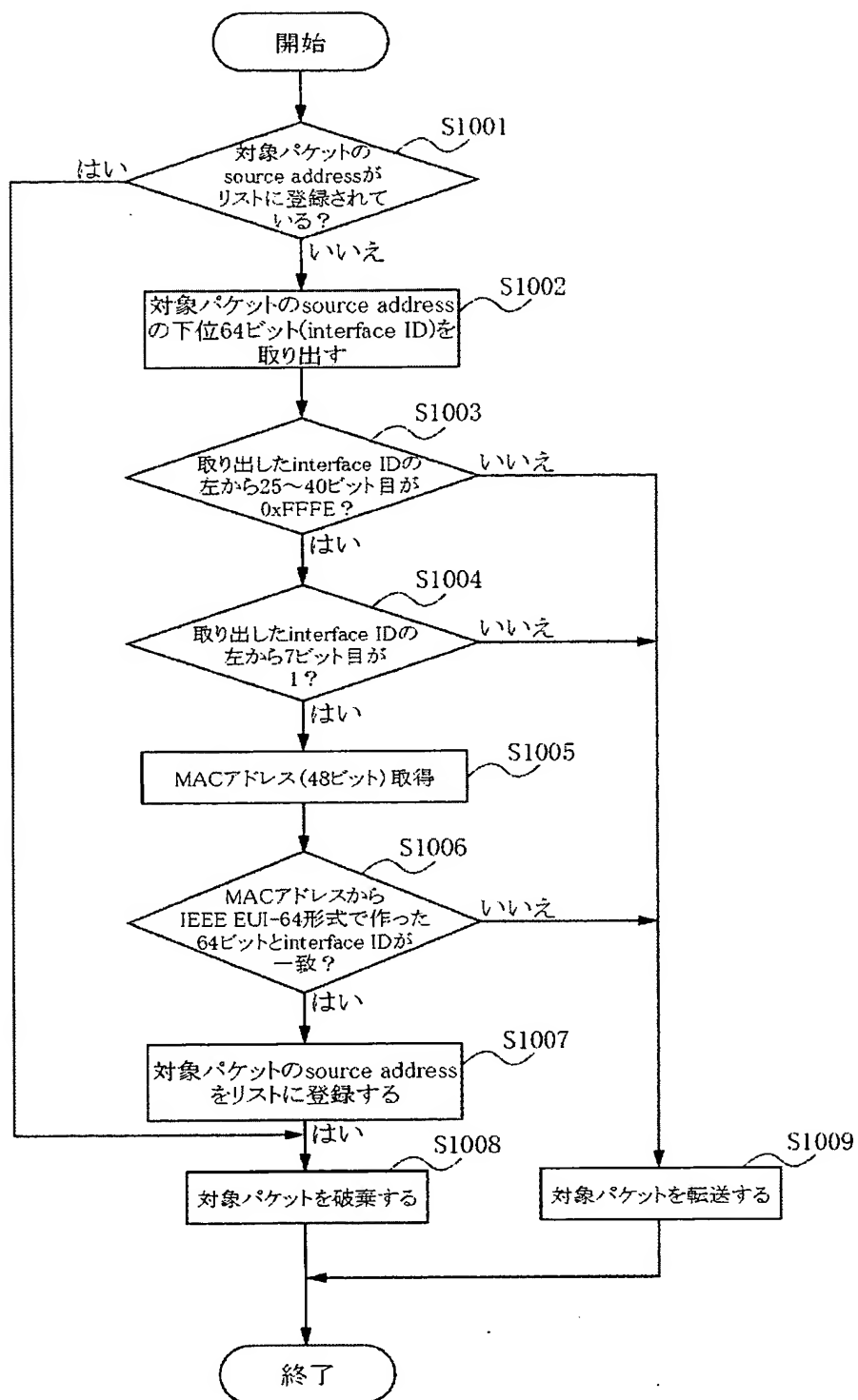
ホストがアドレス自動設定を終えるまでの動作フローチャート

【図 10】



ホストがDHCPでアドレスを取得するまでの動作フローチャート

【図 11】



転送判断の動作フローチャート

【書類名】 要約書

【要約】

【課題】 IPv6 装置が装置固有の識別情報を含む IEEE EUI-64 形式のアドレスを使うと、それらの通信をモニターされてプライバシーが侵害される可能性がある。

【解決手段】 IPv6 装置が使用希望または使用する IPv6 アドレスが匿名アドレス (temporary address) であるか否かを、その装置のデータリンク層の MAC アドレスから IEEE EUI-64 形式で生成したアドレスと比較して判断するノードまたはルーター 202 を、装置と同じサブネット 207 に設ける。IEEE EUI-64 形式のアドレスを使用希望する場合はそれが既に使用されている旨のメッセージをノードが送出して、装置にそのアドレスを使用させない。あるいは、そのアドレスを含むパケットか否かをルーター 202 が判断して、当該パケットの場合は破棄し、ネットワーク外部へ転送しない。

【選択図】 図 2

特願 2 0 0 3 - 1 5 2 8 3 4

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 1 0 0 7]

1. 変更年月日

1 9 9 0 年 8 月 3 0 日

[変更理由]

新規登録

住 所

東京都大田区下丸子 3 丁目 3 0 番 2 号

氏 名

キャノン株式会社